

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019110

International filing date: 21 December 2004 (21.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-433903
Filing date: 26 December 2003 (26.12.2003)

Date of receipt at the International Bureau: 17 February 2005 (17.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

24.12.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 2 月 2 6 日
Date of Application:

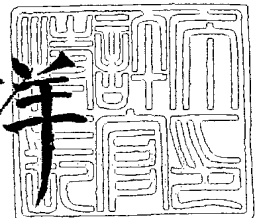
出 願 番 号 特 願 2 0 0 3 - 4 3 3 9 0 3
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 4 3 3 9 0 3]

出 願 人 松 下 電 器 産 業 株 式 有 限 公 司
Applicant(s):

2 0 0 5 年 2 月 4 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



出証番号 出証特 2 0 0 5 - 3 0 0 6 7 8 4

【書類名】 特許願
【整理番号】 2048150070
【提出日】 平成15年12月26日
【あて先】 特許庁長官 殿
【国際特許分類】 G09C 5/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 布田 裕一
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100090446
 【弁理士】
 【氏名又は名称】 中島 司朗
【手数料の表示】
 【予納台帳番号】 014823
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9003742

【書類名】特許請求の範囲

【請求項 1】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムであって、

前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、

前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とする鍵発行システム。

【請求項 2】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムであって、

前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、

前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、

前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とする鍵発行システム。

【請求項 3】

前記証明書発行サーバは、さらに、前記公開鍵が前記発行識別子に基づいた前記素数を用いて生成されているかを判定する鍵判定部を備えること

を特徴とする請求項 2 記載の鍵発行システム。

【請求項 4】

前記素数生成部は、第 1 素数 q 、乱数 R 、前記発行識別子情報 $ID I$ 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数 N を生成すること

を特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の鍵発行システム。

【請求項 5】

前記素数生成部は、 len ビットの素数を生成し、

$len q \geq len / 2$ を満たす $len q$ ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の鍵発行システム（ここで、

a^x は a の x 乗を示す)。

【請求項 6】

前記素数生成部は、 len ビットの素数を生成し、
 $lenq \geq len/2$ を満たす $lenq$ ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod N$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の鍵発行システム。

【請求項 7】

前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むこと

を特徴とする請求項 1 から請求項 6 のいずれか 1 項に記載の鍵発行システム。

【請求項 8】

前記単射関数 f は、前記発行識別子情報 $ID I$ と前記乱数 R を用いて、 $f(ID I, R) = ID I || R$ であること

を特徴とする請求項 1 から 7 記載の鍵発行システム（ここで、 $a || x$ は a と x の連結を示す）。

【請求項 9】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置であって、

前記端末装置は、素数を含む前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、

前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、

前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていること

を特徴とする端末装置。

【請求項 10】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置であって、

前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、

前記秘密鍵は発行識別子情報 $ID I$ に基づいて生成された素数を含み、

前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていること

を特徴とする端末装置。

【請求項 11】

前記素数は、第 1 素数 q 、乱数 R 、前記発行識別子情報 $ID I$ 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表されること

を特徴とする請求項 9 または請求項 10 記載の端末装置。

【請求項 12】

前記単射関数 f は、前記発行識別子情報 $ID I$ と前記乱数 R を用いて、 $f(ID I, R)$

) = $ID I || R$ であること

を特徴とする請求項 9 から請求項 11 のいずれか 1 項に記載の端末装置。

【請求項 13】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバであって、

前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とする鍵発行サーバ。

【請求項 14】

前記素数生成部は、第 1 素数 q 、乱数 R 、前記発行識別子情報 $ID I$ 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数 N を生成すること

を特徴とする請求項 13 記載の鍵発行サーバ。

【請求項 15】

前記素数生成部は、 len ビットの素数を生成し、

$len q \geq len / 2$ を満たす $len q$ ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 13 記載の鍵発行サーバ。

【請求項 16】

前記素数生成部は、 len ビットの素数を生成し、

$len q \geq len / 2$ を満たす $len q$ ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 13 記載の鍵発行サーバ。

【請求項 17】

前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むこと

を特徴とする請求項 13 から請求項 16 のいずれか 1 項に記載の鍵発行サーバ。

【請求項 18】

前記単射関数 f は、前記発行識別子情報 $ID I$ と前記乱数 R を用いて、 $f(ID I, R)$) = $ID I || R$ であること

を特徴とする請求項 13 から 17 記載の鍵発行サーバ。

【請求項 19】

素数を生成する素数生成装置であって、
前記素数生成装置は、発行識別子を生成する発行識別子生成部と、前記発行識別子情報 I D I に基づいて素数を生成する素数生成部と、を備えること
を特徴とする素数生成装置。

【請求項 20】

前記素数生成部は、第 1 素数 q 、乱数 R 、前記発行識別子情報 I D I 及び、前記発行識別子情報 I D I と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(I D I, R) \times q + 1$ で表される素数 N を生成すること
を特徴とする請求項 19 記載の素数生成装置。

【請求項 21】

前記素数生成部は、 len ビットの素数を生成し、
 $len_q \geq len / 2$ を満たす len_q ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 I D I、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 I D I と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(I D I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 19 記載の素数生成装置。

【請求項 22】

前記素数生成部は、 len ビットの素数を生成し、
 $len_q \geq len / 2$ を満たす len_q ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 I D I、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 I D I と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(I D I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 19 記載の素数生成装置。

【請求項 23】

前記単射関数 f は、前記発行識別子情報 I D I と前記乱数 R を用いて、 $f(I D I, R) = I D I \parallel R$ であること

を特徴とする請求項 19 から請求項 22 のいずれか 1 項に記載の素数生成装置。

【請求項 24】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから RSA 暗号の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行方法であって、

前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、

前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とする鍵発行方法。

【請求項 25】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行方法であって、

前記鍵発行サーバは、データを送信する送信部と、データを受信する受信部と、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、

前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、

前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とする鍵発行方法。

【請求項 26】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、

前記プログラムは、素数を含む前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵を格納する公開鍵格納ステップと、を前記端末装置に実行させ、

前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、

前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていること

を特徴とするプログラム。

【請求項 27】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、

前記プログラムは、前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵証明書を格納する公開鍵証明書格納ステップと、を前記端末装置に実行させ、

前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、

前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていること

を特徴とするプログラム。

【請求項 28】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバに実行させるプログラムであって、

前記プログラムは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成ステップと、を前記鍵発行サーバに実行させ、

前記素数生成ステップは、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とするプログラム。

【請求項 29】

素数を生成する素数生成装置に実行させるプログラムであって、
前記プログラムは、発行識別子を生成する発行識別子生成ステップと、前記発行識別子
情報に基づいて素数を生成する素数生成ステップと、を前記素数生成装置に実行させ、
前記素数生成ステップは、前記発行識別子情報と乱数から素数を生成する素数生成単射
関数を用いて前記素数を生成すること
を特徴とするプログラム。

【請求項 3 0】

請求項 2 6 から請求項 2 9 のいずれか 1 項に記載のプログラムを記録した媒体。

【書類名】明細書

【発明の名称】鍵発行システム、鍵発行装置、素数生成装置、鍵発行方法、素数生成方法及び記録媒体

【技術分野】

【0 0 0 1】

本発明は、素因数分解を安全性の根拠として実現する暗号などの情報セキュリティ技術に関する。

【背景技術】

【0 0 0 2】

近年、コンピュータ技術及び通信技術に基づくデータ通信が広く普及してきており、このデータ通信においては、秘密通信方式やデジタル署名方式が用いられる。ここで、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、発信者の身元を証明したりする通信方式である。

【0 0 0 3】

1. 公開鍵暗号方式

これらの秘密通信方式又はデジタル署名方式においては、公開鍵暗号方式とよばれる暗号方式が用いられる。公開鍵暗号方式を用いる秘密通信では、暗号化鍵と復号化鍵とが異なり、復号化鍵は秘密にするが、暗号化鍵は公開する。秘密にする復号化鍵を秘密鍵と呼び、公開する暗号化鍵を公開鍵と呼ぶ。通信相手が多数のとき、共通鍵暗号では通信相手間で鍵をもつ必要があるが、公開鍵暗号では通信相手が一つの固有の鍵をもつだけで通信可能になるため、通信相手が増えても、共通鍵暗号より鍵の数が少なくてよい。このように、公開鍵暗号は多数の通信相手と通信を行うのに適しており、不可欠な基盤技術である。

【0 0 0 4】

公開鍵暗号方式の1種であるRSA暗号方式では、整数の素因数分解問題を解くことが、計算量の上で困難であることを安全性の根拠としている。素因数分解問題とは、 p 、 q を素数とし、整数 $n = p \times q$ とすると、整数 n に対して、素数 p 、 q を求める問題である。ここで、 \times は通常の乗算である。一般に p 、 q が1024ビットの数のように大きい場合は、素因数分解問題が困難である。それにより、RSA暗号方式の公開鍵から秘密鍵を求めることや、秘密鍵を持たないユーザが暗号文から平文を求めることが、困難になる。なお、素因数分解問題については、非特許文献1の144～151ページに詳しく述べられている。

【0 0 0 5】

(素因数分解問題を応用するRSA暗号方式)

ここで、素因数分解問題を応用するRSA暗号方式について説明する。

(1) 鍵の生成

次に示すようにして公開鍵及び秘密鍵を計算する。

・ランダムに大きい素数 p 、 q を選択し、その積 $n = p \times q$ を計算する。

【0 0 0 6】

・ $(p-1)$ 及び $(q-1)$ の最小公倍数 $L = \text{LCM}(p-1, q-1)$ を計算する。
・ L と互いに素で L より小さい自然数 e をランダムに選ぶ。

$1 \leq e \leq L-1$ 、 $\text{GCD}(e, L) = 1$

ここで、 $\text{GCD}(e, L)$ は、 e と L の最大公約数を示している。

・ $e \times d = 1 \pmod{L}$ を満たす d を計算する。 $\text{GCD}(e, L) = 1$ より、このような d は必ず存在する。このようにして、得られた整数 e 及び整数 n が、公開鍵である。また、整数 d が、秘密鍵である。ここで、 $x \pmod{y}$ は、 x を y で割った余りを示す。

【0 0 0 7】

(2) 暗号文の生成

公開鍵である整数 e 及び整数 n を用いて、平文 m に暗号演算を施して暗号文 c を計算する。

$$c = m^e \bmod n$$

なお、この明細書において、演算子 $^$ は、べき乗を示す。例えば、 A^x は、 $x > 0$ のときは A を x 回乗じたものを示す。

【0008】

(3) 復号文の生成

秘密鍵である整数 d を用いて、暗号文 c に復号演算を施して復号文 m' を計算する。

$$m' = c^d \bmod n$$

なお、

$$\begin{aligned} m' &= c^d \bmod n \\ &= (m^e)^d \bmod n \\ &= m^{(e \times d \bmod L)} \bmod n \\ &= m^1 \bmod n \\ &= m \bmod n \end{aligned}$$

であるので、復号文 m' は、平文 m と一致する。

【0009】

また、RSA暗号については、非特許文献2の110～113ページに詳しく説明されている。

上記に示した素因数分解を応用したRSA暗号における公開鍵の生成のステップにおいて、素数生成が行われる。素数生成については、非特許文献3の145～154ページに詳しく説明されている。素数生成方法には、確率的素数生成法と確定的素数生成方法がある。確率的素数生成法により生成される素数は、「素数である確率が高い」数であり、100%素数であるとは限らない。一方、確定的素数生成方法は、確実に素数である数を生成する。確率的素数生成方法及び確定的素数生成方法については、非特許文献2に詳しく説明されている。以下では、確定的素数生成方法について説明する。

【0010】

2. 従来例1—確定的素数生成方法

確定的に素数を生成することができるMaurer法による確定的素数生成方法について説明する。ここで、Maurer法については、非特許文献3の152～153ページに詳しく説明されている。

前記確定的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。あらかじめビットサイズ len_q の素数 q が与えられている。

【0011】

(ステップ1) $(len_q - 1)$ ビットの乱数 R を選択する。なお、乱数 R の先頭ビットは、必ず1となるようにする。

(ステップ2) 数 N を以下の式により計算する。

$$N = 2 \times q \times R + 1$$

(ステップ3) 数 N が素数であるか否かを、次に示す第1判定及び第2判定がともに、成立する場合に、素数と判定する。他の場合に、素数でないと判定する。

【0012】

(第1判定) $2^{(N-1)} = 1 \bmod N$

(第2判定) $GCD(2^{(2R)} - 1, N) = 1$

素数であると判定される場合には、数 N を素数として出力する。素数でないと判定される場合には、ステップ1へ戻って、素数が出力されるまで、処理を繰り返す。

ステップ3で述べられている判定方法は、Pocklingtonの素数判定法とよばれ、非特許文献3の144ページに詳しく述べられている。Pocklingtonの素数判定法では、 $N = 2 \times q \times R + 1$ の q が素数であり、第1判定及び第2判定の結果が真であれば、必ず、 N が素数になる。そのため、確定的に素数であることを判定でき、確定的な素数生成が可能になる。

【0013】

このようにして、Maurer法による確定的素数生成方法では、サイズ $lenq$ の素数 q を基にして、サイズ $2 \times lenq$ の素数 N を生成する。従って、Maurer法による確定的素数生成方法を用いて所定長の素数を生成する場合には、前記所定長以下の素数の生成を繰り返し行う。例えば、512ビット長の素数を生成する場合には、あらかじめ与えられた8ビットの素数を基にして16ビットの素数を生成する。次に、生成した16ビットの素数を基にして32ビットの素数を生成する。次に、生成した32ビットの素数を基にして64ビットの素数を生成する。以下同様の素数生成を繰り返して、512ビットの素数を生成する。

【0014】

なお、前記第2判定を次の判定に代えてもよい。

$$(\text{第3判定}) \quad 2^{(2R)} \neq 1 \pmod{N}$$

上記第3判定方法は、非特許文献4に詳しく述べられている。以降、こちらの判定方法を使用していく。

3. 複数の鍵発行サーバをもつ鍵発行システム

公開鍵暗号の鍵発行システムでは、ユーザが鍵を生成する場合や、鍵発行サーバによりユーザに鍵を発行する場合がある。鍵発行サーバにより鍵を発行する場合、ユーザに鍵を発行するサーバは一台であることが多い。しかし、ユーザが増加すると、上記のような素数生成方法は、複数回べき乗を行うことにより計算量が大きいため、計算時間が大きくなっていく。そこで、鍵発行サーバを複数もち、それぞれで鍵発行をすることにより、計算量の分散を図ることがある。そのとき、各ユーザで同じ素数が鍵となった場合、素因数分解ができるため、安全性が著しく低下する。たとえば、ユーザAの素数を $pA1$ 、 $pA2$ とし、 $nA = pA1 \times pA2$ 、ユーザBの素数を $pB1$ 、 $pB2$ とし、 $nB = pB1 \times pB2$ とする。このとき、 $pA1 = pB1$ であれば、ユーザAは $GCD(pA1, nB)$ を求めることにより、ユーザBの素数の一つが $pA1$ と等しいことがわかり、その結果、 $nB / pA1$ を計算することにより、 $pB2$ も得ることができる。RSA暗号は、素因数分解を安全性の根拠としているため、素因数が判明すると、簡単に解読可能になる。そのため、ユーザAはユーザBの公開鍵で暗号化した暗号文を解ける。また、同様に、ユーザBはユーザAの公開鍵で暗号化した暗号文を解けてしまう。

【特許文献1】特開 2003-5644号公報

【非特許文献1】岡本龍明、太田和夫共編、「暗号・ゼロ知識問題・数論」、共立出版、1990

【非特許文献2】岡本龍明、山本博資、「現代暗号」、産業図書（1997年）

【非特許文献3】A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of applied cryptography", CRC Press, 1997

【非特許文献4】岡本 栄司、「暗号理論入門」、共立出版、1993、21ページ

【発明の開示】

【発明が解決しようとする課題】

【0015】

従来技術では、複数回素数生成を行ったときに素数が一致する可能性があり、それにより、暗号の安全性を著しく低下させるという課題がある。それに対しては、発行済の素数（秘密鍵）と発行した素数を比較することにより、一致しないことを確認できる。しかし、通常の公開鍵暗号のシステムでは、発行した後の公開鍵は鍵発行サーバで管理するが、秘密鍵は機密性が高いため、削除してしまうことが多い。そのため、新たに発行済の素数（秘密鍵）を管理する必要がある。さらに、発行数が10億個程度に大きくなると、比較する時間が大きく現実的でないという課題がある。

【0016】

また、複数の鍵発行サーバで発行した場合、すべての鍵発行サーバで発行した素数が一致させないため、各鍵発行サーバ間で、発行した素数、すなわち、秘密鍵を互いにチェッ

クさせる必要がある。各鍵発行サーバ間で信頼関係がある場合は問題ないが、各鍵発行サーバはそれぞれ別の会社が設置することが多いため、信頼できるとは限らない。さらに、もし、各鍵発行サーバ間で信頼関係がある場合であっても、鍵を発行するたびに、各鍵発行サーバの秘密鍵のデータベースにアクセスするため、各鍵発行サーバ間の通信量が大きくなる。このように各鍵発行サーバ間で互いにチェックすることは現実的でないという課題がある。

【0017】

本発明は、複数回素数生成を行っても、素数が一致しないことを比較することなく、証明できる素数生成方法を提供することを目的とする。

【課題を解決するための手段】

【0018】

上記目的を達成するために、請求項1における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【0019】

請求項2における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【0020】

請求項3における発明は、前記証明書発行サーバは、さらに、前記公開鍵が前記発行識別子に基づいた前記素数を用いて生成されているかを判定する鍵判定部を備えることを特徴とする。

請求項4における発明は、前記素数生成部は、第1素数 q 、乱数 R 、前記発行識別子情報 $ID I$ 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数 N を生成することを特徴とする。

【0021】

請求項5における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len q \geq len / 2$ を満たす $len q$ ビットの第1の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 $ID I$ 、前記第1の素数 q 、前記乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第1の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第2の素数判定部と、を備えることを特徴とする（ここで、 a^x は a の x 乗を示す）。

【0022】

請求項6における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len q$

$\geq \text{len}/2$ を満たす $\text{len}q$ ビットの第1の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 IDI 、前記第1の素数 q 、前記乱数 R 及び、前記発行識別子情報 IDI と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(\text{IDI}, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第1の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $\text{GCD}(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第2の素数判定部と、を備えることを特徴とする。

【0023】

請求項7における発明は、前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする。

請求項8における発明は、前記単射関数 f は、前記発行識別子情報 IDI と前記乱数 R を用いて、 $f(\text{IDI}, R) = \text{IDI} \parallel R$ であることを特徴とする（ここで、 $a \parallel x$ は a と x の連結を示す）。

【0024】

請求項9における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置であって、前記端末装置は、素数を含む前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていることを特徴とする。

【0025】

請求項10における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置であって、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、前記秘密鍵は発行識別子情報 IDI に基づいて生成された素数を含み、前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていることを特徴とする。

【0026】

請求項11における発明は、前記素数は、第1素数 q 、乱数 R 、前記発行識別子情報 IDI 及び、前記発行識別子情報 IDI と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(\text{IDI}, R) \times q + 1$ で表されることを特徴とする。

請求項12における発明は、前記単射関数 f は、前記発行識別子情報 IDI と前記乱数 R を用いて、 $f(\text{IDI}, R) = \text{IDI} \parallel R$ であることを特徴とする。

【0027】

請求項13における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【0028】

請求項14における発明は、前記素数生成部は、第1素数 q 、乱数 R 、前記発行識別子情報 IDI 及び、前記発行識別子情報 IDI と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(\text{IDI}, R) \times q + 1$ で表される素数 N を生成することを特徴とする。

請求項15における発明は、前記素数生成部は、 len ビットの素数を生成し、 $\text{len}q \geq \text{len}/2$ を満たす $\text{len}q$ ビットの第1の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 IDI 、前記第1の素数 q 、前記

乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第 2 の素数判定部と、を備えることを特徴とする。

【0029】

請求項 16 における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len \geq len/2$ を満たす len ビットの第 1 の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えることを特徴とする。

【0030】

請求項 17 における発明は、前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする。

請求項 18 における発明は、前記単射関数 f は、前記発行識別子情報 $ID I$ と前記乱数 R を用いて、 $f(ID I, R) = ID I || R$ であることを特徴とする。

請求項 19 における発明は、素数を生成する素数生成装置であって、前記素数生成装置は、発行識別子を生成する発行識別子生成部と、前記発行識別子情報 $ID I$ に基づいて素数を生成する素数生成部と、を備えることを特徴とする。

【0031】

請求項 20 における発明は、前記素数生成部は、第 1 素数 q 、乱数 R 、前記発行識別子情報 $ID I$ 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数 N を生成することを特徴とする。

請求項 21 における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len \geq len/2$ を満たす len ビットの第 1 の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第 2 の素数判定部と、を備えることを特徴とする。

【0032】

請求項 22 における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len \geq len/2$ を満たす len ビットの第 1 の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 、前記乱数 R 及び、前記発行識別子情報 $ID I$ と乱数 R から整数を生成する単射関数 f を用いて $N = 2 \times f(ID I, R) \times q + 1$ で表される素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えることを特徴とする。

【0033】

請求項 23 における発明は、前記単射関数 f は、前記発行識別子情報 $ID I$ と前記乱数 R を用いて、 $f(ID I, R) = ID I || R$ であることを特徴とする。

請求項 24 における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから RSA 暗号の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行方法であって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵

生成部と、を備え、前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【0034】

請求項25における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行方法であって、前記鍵発行サーバは、データを送信する送信部と、データを受信する受信部と、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【0035】

請求項26における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、前記プログラムは、素数を含む前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵を格納する公開鍵格納ステップと、を前記端末装置に実行させ、前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていることを特徴とする。

【0036】

請求項27における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、前記プログラムは、前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵証明書を格納する公開鍵証明書格納ステップと、を前記端末装置に実行させ、前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていることを特徴とする。

【0037】

請求項28における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバに実行させるプログラムであって、前記プログラムは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成ステップと、を前記鍵発行サーバに実行させ、前記素数生成ステップは、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【0038】

請求項29における発明は、素数を生成する素数生成装置に実行させるプログラムであって、前記プログラムは、発行識別子を生成する発行識別子生成ステップと、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、を前記素数生成装置に実行させ、前記素数生成ステップは、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【0039】

請求項30における発明は、請求項26から請求項29のいずれか1項に記載のプログラムを記録した媒体である。

【発明の効果】

【0040】

これらの構成によると、複数回素数生成を行っても、素数が一致しないことを比較することなく、証明できる素数生成を実現でき、その価値は大きい。

【発明を実施するための最良の形態】

【0041】

(実施の形態1)

本発明に係る1の実施の形態としての素数生成装置1について説明する。

図1は、実施の形態1における素数生成装置の構成を示す図である。

この素数生成装置1は、素数 q 、 q のビットサイズ $\text{len } q$ 、発行識別子情報 IDI 及び発行識別子情報のビットサイズ len IDI が与えられたとき、 q のビットサイズ $\text{len } q$ の2倍のビットサイズ $2 \times \text{len } q$ をもつ素数 N を出力するものである。

【0042】

<素数生成装置1の構成>

素数生成装置1は、乱数生成部11と、素数候補生成部12、第1素数判定部13と、第2素数判定部14を備える。

乱数生成部11は、 $\text{len } q$ を用いて、 $(\text{len } q - \text{len IDI} - 1)$ ビットの乱数 R を生成する。ここで、乱数 R' の最上位ビットは1とする。乱数生成方法は、非特許文献2が詳しい。

【0043】

素数候補生成部12は、 q 及び R' を用いて、以下の式を満たす R と N を生成する。

$$R = f(\text{IDI} \parallel R')$$

$$N = 2 \times R \times q + 1$$

ここで、 f は単射である関数であり、例えば、 $f(\text{IDI} \parallel R') = \text{Enc}(K, \text{IDI} \parallel R')$ である。 $\text{Enc}(K, \text{IDI})$ は鍵 K を用いたときの IDI の共通鍵暗号による暗号文である。共通鍵暗号の暗号化関数は一般的に全単射である。また、 \parallel はビットまたはバイト連結である。

【0044】

第1素数判定部13は、 N を用いて、以下の式の成立を判定する。

$$2^{(N-1)} = 1 \pmod{N} \quad (\text{eq 1})$$

ここで、 $2^{(N-1)}$ は、2の $N-1$ 乗を示している。

第2素数判定部14は、 N と R を用いて、以下の式の成立を判定する。

$$2^{(2R)} \neq 1 \pmod{N} \quad (\text{eq 2})$$

<素数生成装置1の動作>

以下に素数生成装置1の動作を示す。図2にこの動作のフローチャートを示す。

【0045】

ステップS101: 乱数生成部11は、 $(\text{len } q - \text{len IDI} - 1)$ ビットの乱数 R' を生成する。ここで、乱数 R' の最上位ビットは1とする。

ステップS102: 素数候補生成部12は、以下の式を満たす R と N を生成する。

$$R = f(\text{IDI} \parallel R')$$

$$N = 2 \times R \times q + 1$$

ステップS103: 第1素数判定部13は、 $2^{(N-1)} = 1 \pmod{N}$ の成立を判定する。この式が成立する場合は次のステップへ。成立しない場合はステップS101へ。

【0046】

ステップS104: 第2素数判定部14は、 $2^{(2R)} \neq 1 \pmod{N}$ の成立を判定する。この式が成立する場合は N を出力し、終了する。成立しない場合は、ステッ

プ S101 へ。

＜素数生成装置 1 の動作検証＞

第 1 素数判定部及び、第 2 素数判定部は、Pocklington 判定である。Pocklington 判定は、非特許文献 1 の 144 ページ及び非特許文献 4 が詳しい。

【0047】

$N = 2 \times R \times q + 1$ の q が素数であり

$$2^{(N-1)} = 1 \pmod{N}$$

$$2^{(2R)} \neq 1 \pmod{N}$$

の両方が成り立つ場合、 N が素数になるので、素数生成装置 1 は素数を出力する。

また、乱数 R' のビットサイズが $(len q - len ID - 1)$ であるので、 R のビットサイズが $(len q - 1)$ になり、ほとんどの N のビットサイズが $2 \times len q$ になる。ここで、 q や ID などの値によっては、ビットサイズが $2 \times len q - 1$ となる場合がある。その場合は、素数候補生成部 12 で、 R' に 2 を掛けて、それを新たに R' とみなすことにより、 N のビットサイズを $2 \times len q$ になるように設定する。

【0048】

＜実施の形態 1 の効果＞

発行識別子情報 ID が異なれば、出力される素数 N が異なること (*) を以下で述べる。まず、以下の補題を証明し、その補題を用いて (*) を証明する。

(補題) 二つの素数 $p_1 = 2 \times q_1 \times R_1 + 1$, $p_2 = 2 \times q_2 \times R_2 + 1$ に対し、 $p_1 = p_2$ であれば、 $q_1 = q_2$ かつ $R_1 = R_2$ (証明) $p_1 = p_2$ の場合、 q_1 , q_2 : 256 ビットの素数であり、 R_1 , R_2 : 255 ビットであるため、 $q_1 = q_2$ となるのは明らか。また、 $q_1 = q_2$ より、 $R_1 = R_2$ も成り立つ (証明終)。

【0049】

上記補題より、 $p_1 = p_2$ であれば、 $R_1 = R_2$ が成り立つ。 $R_1 = f(IDI_1 || R'_1)$ 、 $R_2 = f(IDI_2 || R'_2)$ とおくと、 $R_1 = R_2$ であり、 f は単射であるため、 $IDI_1 = IDI_2$ である。したがって、この対偶を取ることにより、(*) が成り立つ。以上より、 ID が異なれば必ず素数が異なる。したがって、 ID を毎回変えることで、毎回異なる素数を生成することができる。 ID はカウンタでもよく、発行のたびにインクリメントしていくことで、容易に毎回異なる素数を生成できることになる。したがって、複数回生成した素数が一致しないことを比較することなく、証明できる。

【0050】

(実施の形態 2)

本発明に係る 2 の実施の形態としての素数生成装置 2 について、説明する。

図 3 は、実施の形態 2 における素数生成装置の構成を示す図である。

この素数生成装置 2 は、素数 q_1 、 q_1 のビットサイズ $len q_1$ 、発行識別子情報 ID 及び発行識別子情報のビットサイズ $len ID$ が与えられたとき、 q_1 のビットサイズ $len q_1$ の 4 倍のビットサイズ $4 \times len q_1$ をもつ素数を出力するものである。

【0051】

＜素数生成装置 2 の構成＞

素数生成装置 2 は、実施の形態 1 と同様の第 1 素数判定部 13 と、第 2 素数判定部 14 と、実施の形態 1 と異なる素数シード生成部 21 と、乱数生成部 22 と、素数候補生成部 23 と、を備える。

素数シード生成部 21 は、素数生成装置 1 を用いて、 q_1 のビットサイズの 2 倍のビットサイズをもつ素数 q_2 を生成する。

【0052】

乱数生成部 22 は、 $len q_1$ を用いて、 $(2 \times len q_1 - len ID - 1)$ ビットの乱数 R' を生成する。ここで、 R' の最上位ビットは 1 とする。

素数候補生成部 23 は、 q_2 及び R' を用いて、以下の式を満たす R と N を生成する。

$$R = IDI \times R'$$

【0053】

$$N = 2 \times R \times q^2 + 1$$

<素数生成装置2の動作>

以下に素数生成装置2の動作を示す。図4にこの動作のフローチャートを示す。

ステップS201: 素数シード生成部21は、素数 q^2 を生成する。

ステップS202: 乱数生成部22は、 $(2 \times \text{len } q^1 - \text{len } \text{IDI} - 1)$ ビットの乱数 R' を生成する。ここで、 R' の最上位ビットは1とする。

【0054】

ステップS203: 素数候補生成部23は、 R と N を計算する。

ステップS204: 第1素数判定部13は、 $2^{(N-1)} \equiv 1 \pmod{N}$ の成立を判定する。この式が成立する場合は次のステップS205へ。成立しない場合はステップS202へ。

ステップS205: 第2素数判定部14は、 $2^{(2R)} \not\equiv 1 \pmod{N}$ の成立を判定する。この式が成立する場合は N を出力し、終了する。成立しない場合は、ステップS202へ。

【0055】

<実施の形態2の効果>

発行識別子情報 IDI が異なれば、出力される素数 N が異なることが実施の形態1と同様にいえる。以下に説明する。素数生成装置2で生成した二つの素数 $N_1 = 2 \times q^1_1 \times R_1 + 1$ 、 $N_2 = 2 \times q^1_2 \times R_2 + 1$ に対し、二つの素数の発行識別子 IDI が異なれば、 $q^1_1 \neq q^1_2$ であるため、先に述べた補題より $N_1 \neq N_2$ である。以上より、 IDI が異なれば必ず素数が異なる。

【0056】

また、生成された素数 N に対して、 $N-1$ は必ず発行識別子情報 IDI で割り切れる。なぜなら、 $N-1 = 2 \times q^2 \times \text{IDI} \times R'$ が成り立つためである。したがって、生成された素数 N に対し、 $N-1$ が発行識別子情報 IDI で割り切れるか否かで、素数生成装置2を用いて素数が生成されたかを確認することができる。

(実施の形態3)

本発明に係る3の実施の形態としての素数生成装置3について、説明する。

【0057】

図5は、実施の形態3における素数生成装置の構成を示す図である。

この素数生成装置3は、素数 q 、 q のビットサイズ $\text{len } q$ 、発行識別子情報 IDI 及び発行識別子情報のビットサイズ $\text{len } \text{IDI}$ が与えられたとき、 q のビットサイズ $\text{len } q$ の2倍のビットサイズ $2 \times \text{len } q$ をもつ素数を出力するものである。

<素数生成装置3の構成>

素数生成装置3は、実施の形態1と同様の第1素数判定部13と、第2素数判定部14と、実施の形態1と異なる識別子素数生成部31と、乱数生成部32と、素数候補生成部33と、を備える。

【0058】

識別子素数生成部31は、予め与えられた素数 q_g と発行識別子情報 IDI より、素数 $p_{\text{IDI}} = g_p(\text{IDI}, q_g)$ を生成する。 g_p は発行識別子 IDI と素数 q_g から一意的に素数を生成する素数生成関数である。例えば、 $g_p(\text{IDI}, q_g)$ は、以下のよう求める。 $c=0$ として、 $2 \times q_g \times f(\text{IDI} \parallel c) + 1$ が素数であるかを判定する。素数である場合は、 $g_p(\text{IDI}, q_g) = 2 \times q_g \times f(\text{IDI} \parallel c) + 1$ とする。素数でなければ、 c に1加算して $2 \times q_g \times f(\text{IDI} \parallel c) + 1$ が素数であるかを判定する。素数であれば、 $g_p(\text{IDI}, q_g) = 2 \times q_g \times f(\text{IDI} \parallel c) + 1$ とする。素数でなければ、 c に1加算して同様の判定を行い素数になるまで繰り返す。

【0059】

また、 $\text{len } q_g$ は q_g のビットサイズである。このように関数 g_p を定義するとき、 q_g を保持していれば、発行識別子情報 IDI に対して、何回素数生成関数により素数を

生成しても、同じ素数を生成可能である。

乱数生成部 32 は、 $(1 \text{ en } q - 2 \times 1 \text{ en } q \text{ g} - 1)$ ビットの乱数 R を生成する。ここで、R の最上位ビットは 1 とする。

【0060】

素数候補生成部 33 は、素数 q, p I D I 及び乱数 R を用いて、以下の式を満たす N を生成する。

$$N = 2 \times R \times q \times p \text{ I D I} + 1$$

<素数生成装置 3 の動作>

以下に素数生成装置 3 の動作を示す。図 6 にこの動作のフローチャートを示す。

【0061】

ステップ S301: 識別子素数生成部 31 は、素数 p I D I を生成する。

ステップ S302: 乱数生成部 32 は、乱数 R を生成する。

ステップ S303: 素数候補生成部 33 は、 $N = 2 \times R \times q \times p \text{ I D I} + 1$ に設定する。

ステップ S304: 第 1 素数判定部 13 は、 $2^{(N-1)} = 1 \text{ mod } N$ の成立を判定する。この式が成立する場合は次のステップ S305 へ。成立しない場合は、ステップ S302 へ。

【0062】

ステップ S305: 第 2 素数判定部 14 は、 $2^{(2R)} \neq 1 \text{ mod } N$ の成立を判定する。この式が成立する場合は N を出力し、終了する。成立しない場合は、ステップ S302 へ。

<実施の形態 3 の効果>

発行識別子情報 I D I が異なれば、素数が異なることが実施の形態 1、2 と同様にいえる。

【0063】

また、生成された素数 N に対して、 $N-1$ は、素数生成関数により生成される $g \text{ p} (I \text{ D I}, q \text{ g})$ で割り切れる。したがって、生成された素数が、 $g \text{ p} (I \text{ D I}, q \text{ g})$ で割り切れるか否かで素数生成装置 3 を用いて素数が生成されたかを確認することができる。

(実施の形態 4)

本発明に係る 4 の実施の形態としての鍵発行システム 4 について、説明する。

図 7 は、実施の形態 4 における鍵発行システム 4 の構成を示す図である。本システムは、鍵発行サーバ A 41、B 42、C 43 と、証明書発行サーバ 44 と、端末装置 451、452、453、...、45n から構成される。n は自然数であり、例えば 1000 である。この場合、端末装置が 1000 台存在することになる。

【0064】

<鍵発行サーバ A 41、B 42、C 43 の構成>

鍵発行サーバ A 41、B 42、C 43 は同じ構成であるため、以下では代表して鍵発行サーバ A 41 の構成を示す。鍵発行サーバ A 41、B 42、C 43 にはそれぞれ、予め識別子: S I D A、S I D B、S I D C が与えられている。

鍵発行サーバ A 41 は、RSA 暗号における秘密鍵及び公開鍵を生成し、公開鍵を証明書発行サーバへ送信し、公開鍵証明書を受信した後、端末装置へ送信する。

【0065】

鍵発行サーバ A 41 は、送信部 4101 と、受信部 4102 と、識別子生成部 4103、識別子格納部 4104 と、素数生成部 4105 と、秘密鍵判定部 4106 と、鍵生成部 4107 と、秘密鍵格納部 4108 と、公開鍵格納部 4109 と、証明書格納部 4110 を備える (図 8 参照)。

送信部 4101 は、端末装置 45i ($i = 1 \sim n$) へ生成した秘密鍵及び公開鍵を、証明書発行サーバ 44 へ公開鍵を送信する。

【0066】

受信部 4102 は、端末装置 45i から鍵生成要求情報を、証明書発行サーバ 44 から

公開鍵証明書 *Cert* を受信する。公開鍵証明書については、証明書発行サーバ 44 の構成の説明で述べる。

識別子生成部 4103 は、端末装置 45 i 用に素数の発行識別子情報 *IDI* を生成し、識別子格納部 4104 に格納する。発行識別子情報 *IDI* は、予め与えられた各鍵発行サーバに対応する識別子: *SID* (*A41* は *SIDA*、*B42* は *SIDB*、*C43* は *SIDC*) と発行識別子: *PID* からなる。例えば、 $IDI = SID || PID$ とする。ここで、 $||$ はビットまたはバイト連結である。発行識別子は例えば、1 から発行順に数字を割り当て、発行するたびにインクリメントする。

【0067】

識別子格納部 4104 は、素数の発行識別子情報 *IDI* を格納する。

素数生成部 4105 は、512 ビット素数を生成する。なお、ここでは鍵長が 1024 ビットの *RSA* を想定しているため、512 ビット素数を生成するとしたが、鍵長を len ビットとして、 $len/2$ ビットの素数を生成するとしてもよい。

(素数生成部 4105 の構成及び動作)

素数生成部 4105 は、第 1 の素数生成部 41051 と、第 2 の素数生成部 41052 と、を備える (図 9 参照)。

【0068】

第 1 の素数生成部 41051 は、128 ビットの素数 q を生成する。素数の生成方法は従来の方法を用いる。従来の方法については、特許文献 1 及び非特許文献 3 が詳しい。

第 2 の素数生成部 41052 は、128 ビット素数 q と、 q のビットサイズ 128 と、発行識別子情報 *IDI* を用いて、512 ビットの素数 N を生成する。第 2 の素数生成部 41052 は、素数生成装置 2 を用いて、素数 N を生成する。

【0069】

秘密鍵判定部 4106 は、2 回の素数生成部 4105 の処理を実行して出力された素数 $p1$ と $p2$ が一致しているかを比較する。

鍵生成部 4107 は、秘密鍵格納部 4108 に格納されている秘密鍵 $p1$ 、 $p2$ の積 $n = p1 \times p2$ を計算し、さらに、乱数 e を生成し、それらの n と e の組 $PK = (n, e)$ を公開鍵とする。

【0070】

その後、 $e \times d = 1 \pmod{L}$ を満たす d を計算し秘密鍵とする。ここで、 $L = LCM(p1-1, p2-1)$ である。 $LCM(p1-1, p2-1)$ は $p1-1$ と $p2-1$ の最小公倍数を示す。

秘密鍵格納部 4108 は、素数生成部 4105 で生成した 2 つの素数 $p1$ 、 $p2$ と鍵生成部で作成した d の組 $SK = (p1, p2, d)$ を秘密鍵として格納する。

【0071】

公開鍵格納部 4109 は、鍵生成部 4107 で生成した公開鍵 PK を格納する。

証明書格納部 4110 は、証明書発行サーバ 44 が送信した公開鍵証明書 *Cert* を格納する。

<鍵発行サーバ *A41*、*B42*、*C43* の動作>

鍵発行サーバ *A41*、*B42*、*C43* の動作は同様であるため、以下に代表して鍵発行サーバ *A41* の動作を示す。ここでは、端末装置 45 i (i は 1 から n のいずれかの数) から鍵発行依頼情報が送信された場合の動作を示している。図 10 にこの動作のフローチャートを示す。

【0072】

ステップ *S401*: 受信部 412 は、端末装置 45 i より送信された鍵発行依頼情報を受信する。

ステップ *S402*: 識別子生成部 413 は、発行識別子情報: *IDI* を生成し、識別子格納部 414 に格納する。

ステップ *S403*: 素数生成部 415 は、素数 $p1$ を生成する。

【0073】

ステップS404:素数生成部415は、素数 p_2 を生成する。

ステップS405:秘密鍵判定部416は、素数 p_1 と p_2 が $p_1 = p_2$ を満たすかを判定する。 $p_1 = p_2$ の場合は、ステップS404へ。それ以外は、秘密鍵格納部418に格納する。次のステップS406へ。

ステップS406:鍵生成部417は、 $n = p_1 \times p_2$ を計算する。また、鍵生成部417は、乱数 e を生成し、 n と e の組 $PK = (n, e)$ を公開鍵として公開鍵格納部419に格納する。さらに、鍵生成部417は、 $e \times d = 1 \pmod{L}$ を満たす d を計算し、 p_1 、 p_2 と d の組 $SK = (p_1, p_2, d)$ を秘密鍵として秘密鍵格納部418に格納する。

【0074】

ステップS407:送信部411は、公開鍵格納部419に格納されている公開鍵 PK 及び識別子格納部414に格納されている発行識別子情報 IDI を証明書発行サーバ44へ送信する。

ステップS408:受信部412は、証明書発行サーバ44より送信された公開鍵証明書 $Cert$ を受信する。

【0075】

ステップS409:送信部411は、秘密鍵格納部418に格納されている秘密鍵 $SK = (p_1, p_2, d)$ と、公開鍵証明書 $Cert$ を端末装置45iへ送信する。終了する。

<証明書発行サーバ44の構成>

証明書発行サーバ44は、送信部441と、受信部442と、秘密鍵格納部443と、発行公開鍵確認部444と、発行公開鍵格納部445と、発行識別子情報格納部446と、公開鍵証明書生成部447と、公開鍵証明書格納部448と、を備える(図11参照)。

【0076】

送信部441は、証明書 $Cert$ を鍵発行サーバA41、B42または、C43へ送信する。

受信部442は、鍵発行サーバA41、B42または、C43から公開鍵 n 、 e を受信する。

秘密鍵格納部443は、証明書発行サーバ44の秘密鍵 $SKCA$ を格納する。

【0077】

発行公開鍵確認部444は、鍵発行サーバA41、B42またはC43から受信した公開鍵 $PK = (n, e)$ と発行識別子情報 IDI を用いて、公開鍵 $PK = (n, e)$ が発行識別子情報 IDI を用いて生成されたかを確認する。具体的には、 $n-1$ が IDI で割り切れるか否かでチェックする。割り切れる場合は、公開鍵 $PK = (n, e)$ が発行識別子情報 IDI で生成されたと判断し、それ以外は発行識別子情報 IDI で生成されていないと判断する。

【0078】

発行公開鍵格納部445は、鍵発行サーバA41、B42またはC43から受信した公開鍵 $PK = (n, e)$ を格納する。

発行識別子情報格納部446は、鍵発行サーバA41、B42またはC43から受信した発行識別子情報 IDI を格納する。

公開鍵証明書生成部447は、公開鍵 PK と発行識別子情報 IDI に対する公開鍵証明書 $Cert$ を、秘密鍵格納部443に格納されている秘密鍵 $SKCA$ を用いて生成する。具体的には、例えば、 $Cert = n || e || IDI || Sig(SKCA, n || e || IDI)$ とする。ここで、 $Sig(K, D)$ はデータ D に対する鍵 K を用いたときの署名データである。また、 $||$ はビットまたはバイトの連結である。

【0079】

公開鍵証明書格納部448は、公開鍵証明書 $Cert$ を格納する。

<証明書発行サーバ44の動作>

以下に証明書発行サーバ44の動作を示す。ここでは、証明書を発行する先を鍵発行サーバA41として動作を示す。なお、他の鍵発行サーバ(B42、C43)を発行先の場合も同様の動作を行う。図12にこの動作のフローチャートを示す。

【0080】

ステップS501:受信部442は、鍵発行サーバA41から送信された公開鍵 $PK=(n, e)$ と発行識別子情報 IDI を受信する。

ステップS502:発行公開鍵確認部444は、公開鍵 $PK=(n, e)$ が発行識別子情報 IDI を用いて生成されたかを確認する。公開鍵 $PK=(n, e)$ が発行識別子情報 IDI で生成されていると判断した場合は、次のステップS503へ。それ以外は、システムを終了する。

【0081】

ステップS503:発行公開鍵格納部445は、公開鍵 $PK=(n, e)$ を、発行識別子情報格納部446は、発行識別子情報 IDI をそれぞれ格納する。

ステップS504:公開鍵証明書生成部447は、公開鍵 $PK=(n, e)$ と発行識別子情報 IDI に対する公開鍵証明書 $Cert$ を生成し、公開鍵証明書格納部448に格納する。

【0082】

ステップS505:送信部441は、公開鍵証明書格納部448に格納されている公開鍵証明書 $Cert$ を鍵発行A41へ送信し、終了する。

<端末装置45i (i=1~n)の構成>

端末装置451、452、453、...、45nはそれぞれ、同じ構成をしているため、以下では代表して、端末装置45iの構成を示す。

【0083】

端末装置45iは、送信部45i1と、受信部45i2と、秘密鍵格納部45i3と、公開鍵格納部45i4と、発行識別子情報格納部45i5と、を備える(図13参照)。

送信部45i1は、鍵発行依頼情報を鍵発行サーバA41、B42、C43のいずれかへ送信する。鍵発行依頼情報は、例えば、端末装置45iを示す識別子情報などである。

受信部45i2は、鍵発行サーバA41、B42、C43のいずれかから送信された秘密鍵 $SK=(p1, p2, d)$ 、公開鍵 $PK=(n, e)$ と、発行識別子情報 IDI を受信する。

【0084】

秘密鍵格納部45i3は、秘密鍵 $SK=(p1, p2, d)$ を格納する。

公開鍵証明書格納部45i4は、公開鍵証明書 $Cert$ を格納する。

<端末装置45iの動作>

以下に端末装置45iの動作を示す。ここでは、鍵発行サーバA41に鍵発行を依頼する場合の動作を示している。図14にこの動作のフローチャートを示す。

【0085】

ステップS601:送信部45i1は、鍵発行依頼情報を鍵発行サーバA41へ送信する。

ステップS602:受信部45i2は、鍵発行サーバA41より送信された秘密鍵 $SK=(p1, p2, d)$ 、公開鍵証明書 $Cert$ を受信する。

ステップS603:秘密鍵格納部45i3は、秘密鍵 $SK=(p1, p2, d)$ を格納する。

【0086】

ステップS604:公開鍵証明書格納部45i4は、公開鍵証明書 $Cert$ を格納し、終了する。

<鍵発行システム4の動作>

以下に鍵発行システム4の動作を示す。以下では、鍵発行サーバA41が端末装置45iに鍵を発行するときの動作を示す。端末装置45iは、まず、鍵発行依頼情報を鍵発行サーバA41へ送信する。鍵発行サーバA41は、鍵発行依頼情報を受信した後、発行識

別子情報 $ID I$ を作成する。その後、鍵発行サーバ $A 4 1$ は秘密鍵 $SK = (p 1, p 2, d)$ 、公開鍵証明書 $PK = (n, e)$ を生成する。さらに、鍵発行サーバ $A 4 1$ は、公開鍵 $PK = (n, e)$ と発行識別子情報 $ID I$ を証明書発行サーバ $4 4$ へ送信する。証明書発行サーバ $4 4$ は、公開鍵 PK に対応する秘密鍵 SK に含まれる素数 $p 1$ 、 $p 2$ が発行識別子情報 $ID I$ を用いて生成されているかを判定する。証明書発行サーバ $4 4$ は、判定結果が肯定的な場合に、公開鍵 PK に対する公開鍵証明書 $Cert$ を生成し、公開鍵証明書 $Cert$ を鍵発行サーバ $A 4 1$ へ送信する。鍵発行サーバ $A 4 1$ は、秘密鍵 $SK = (p 1, p 2, d)$ と公開鍵証明書 $Cert$ を端末装置 $4 5 i$ へ送信する。端末装置 $4 5 i$ は、秘密鍵 SK 、公開鍵証明書 $Cert$ を格納し、システムを終了する。

【0087】

＜実施の形態 4 の効果＞

実施の形態 2 と同様の理由で、鍵発行サーバは各端末装置に異なる秘密鍵を発行できる。また、発行識別子情報 $ID I$ に鍵発行サーバの識別子を含んでいるため、各鍵発行サーバごとに異なる秘密鍵を発行できることが証明できる。

証明書発行サーバは、鍵発行サーバが正しく発行識別子情報 $ID I$ を用いて生成しているかを確認することができる。なぜなら、秘密鍵である素数 $p 1$ 、 $p 2$ はそれぞれ、素数 $q 1$ 、 $q 2$ 、乱数 $R 1'$ 、 $R 2'$ 、発行識別子情報 $ID I$ を用いて、 $p 1 = 2 \times q 1 \times ID I \times R 1' + 1$ 、 $p 2 = 2 \times q 2 \times ID I \times R 2' + 1$ を満たすため、

$$\begin{aligned} n &= p 1 \times p 2 = (2 \times q 1 \times ID I \times R 1' + 1) \times (2 \times q 2 \times ID I \times R 2' + 1) \\ &= 4 \times q 1 \times q 2 \times R 1' \times R 2' \times ID I^2 + 2 \times q 1 \times ID I \times R 1' + 2 \times q 2 \times ID I \times R 2' + 1 \\ &= ID I \times (4 \times q 1 \times q 2 \times R 1' \times R 2' \times ID I + 2 \times q 1 \times R 1' + 2 \times q 2 \times R 2') + 1 \end{aligned}$$

となる。そのため、 $n - 1$ は $ID I$ で割り切れるため、 $n - 1$ が $ID I$ で割り切れることを確認することで、素数 $p 1$ 、 $p 2$ が正しく発行識別子情報 $ID I$ を用いて生成しているかを確認することができる。

【0088】

なお、以下の確認方法により、不正を働いた端末の情報を得ることができる。不正を働いた端末の秘密鍵 $p 1$ 、 $p 2$ が判明したとする。また、不正の追跡者は、発行識別子情報と端末の対応表と持っているとする。 $p 1 - 1$ 、 $p 2 - 1$ は共に発行識別子情報 $ID I$ で割り切れる。そのため、 $GCD(p 1 - 1, p 2 - 1)$ は発行識別子情報で割り切れる。したがって、 $GCD(p 1 - 1, p 2 - 1)$ の素因数を調べることにより、不正の追跡者は、取りうる発行識別子情報を限定でき、発行識別子情報を知る、すなわち、端末を特定するための助けとなる。

【0089】

(変形例)

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。例えば、以下のような場合も本発明に含まれる。

(1) 先にも述べたが、実施の形態 4 における、生成する秘密鍵である素数のビットサイズは 512 に限らない。1024 であっても、2048 であってもよい。また、素数情報生成部で生成する素数も同様に 256 ビットに限らない。

【0090】

(2) 実施の形態 1、2 または 3 の素数生成装置を素数生成手段として用いて、整数 len と発行識別子情報 $ID I$ を入力とし、 len ビットの素数を出力する素数生成装置としてもよい。また、実施の形態 4 の素数情報生成部で使用する素数生成方法は、実施の形態 1、2 または 3 の素数生成装置であってもよい。

(3) 素数に発行識別子情報を含ませる方法は、実施の形態に限らない。例えば、下位 $len ID I$ ビットが $ID I$ である素数を生成・発行するとしてもよい。

【0 0 9 1】

(4) 鍵発行サーバは 3 台以外の何台であってもよい。

【産業上の利用可能性】

【0 0 9 2】

これらの構成によると、複数回素数生成を行っても、素数が一致しないことを比較することなく、証明できる素数生成を実現できる。

【図面の簡単な説明】

【0 0 9 3】

【図 1】 本発明に係る 1 個の実施の形態としての素数生成装置 1 の構成を示すブロック図

【図 2】 素数生成装置 1 の動作を示すフローチャート

【図 3】 本発明に係る 1 個の実施の形態としての素数生成装置 2 の構成を示すブロック図

【図 4】 素数生成装置 2 の動作を示すフローチャート

【図 5】 本発明に係る 1 個の実施の形態としての素数生成装置 3 の構成を示すブロック図

【図 6】 素数生成装置 3 の動作を示すフローチャート

【図 7】 本発明に係る 1 個の実施の形態としての鍵発行システム 4 の構成を示すブロック図

【図 8】 鍵発行サーバ A 4 1 の構成を示す図

【図 9】 素数生成部 4 1 0 5 の構成を示す図

【図 1 0】 鍵発行サーバ A 4 1 の動作を示すフローチャート

【図 1 1】 証明書発行サーバ 4 4 の構成を示す図

【図 1 2】 証明書発行サーバ 4 4 の動作を示すフローチャート

【図 1 3】 端末装置 4 5 i の構成を示す図

【図 1 4】 端末装置 4 5 i の動作を示すフローチャート

【符号の説明】

【0 0 9 4】

1、2、3 素数生成装置

1 1、2 2、3 2 乱数生成部

1 2、2 3、3 3 素数候補生成部

1 3 第 1 素数判定部

1 4 第 2 素数判定部

2 1 素数シード生成部

3 1 識別子素数生成部

4 鍵発行システム

4 1 鍵発行サーバ A

4 1 0 1、4 4 1、4 5 i 1 送信部

4 1 0 2、4 4 2、4 5 i 2 受信部

4 1 0 3 識別子生成部

4 1 0 4 識別子格納部

4 1 0 5 素数生成部

4 1 0 5 1 第 1 の素数生成部

4 1 0 5 2 第 2 の素数生成部

4 1 0 6 秘密鍵判定部

4 1 0 7 鍵生成部

4 1 0 8、4 4 3、4 5 i 3 秘密鍵格納部

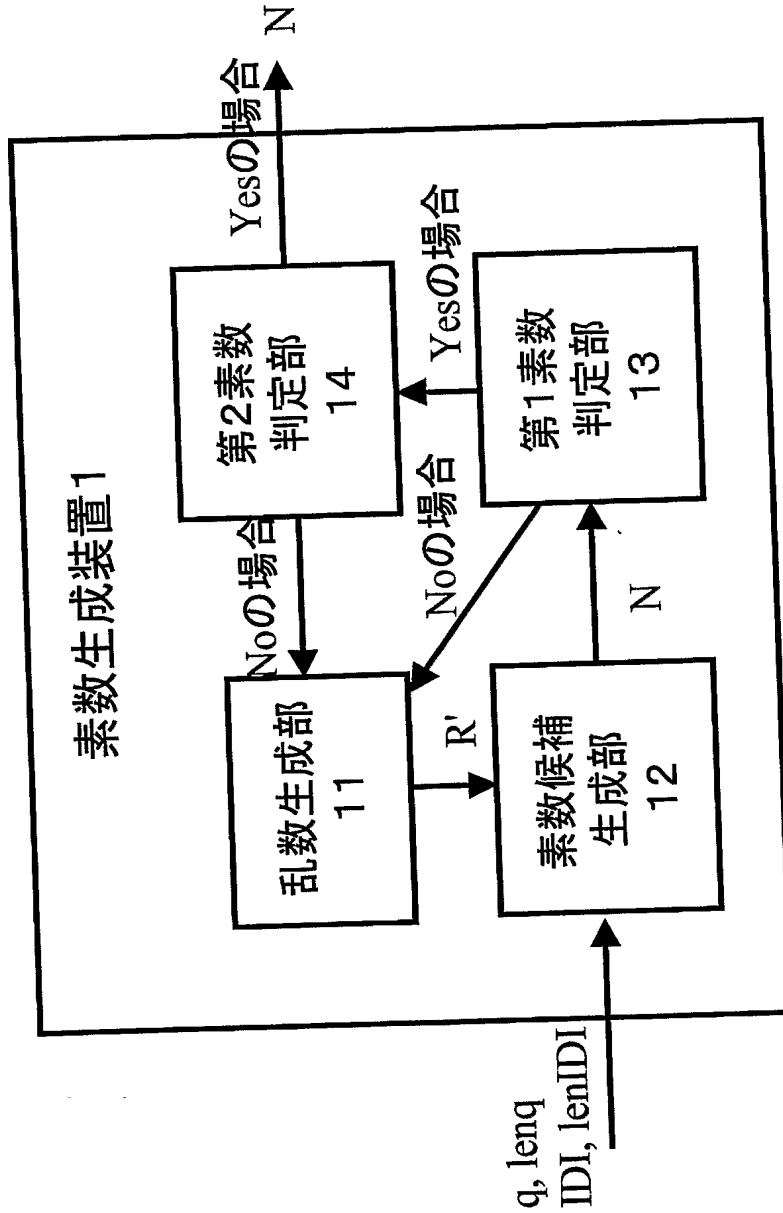
4 1 0 9 公開鍵格納部

4 1 1 0、4 5 i 4 公開鍵証明書格納部

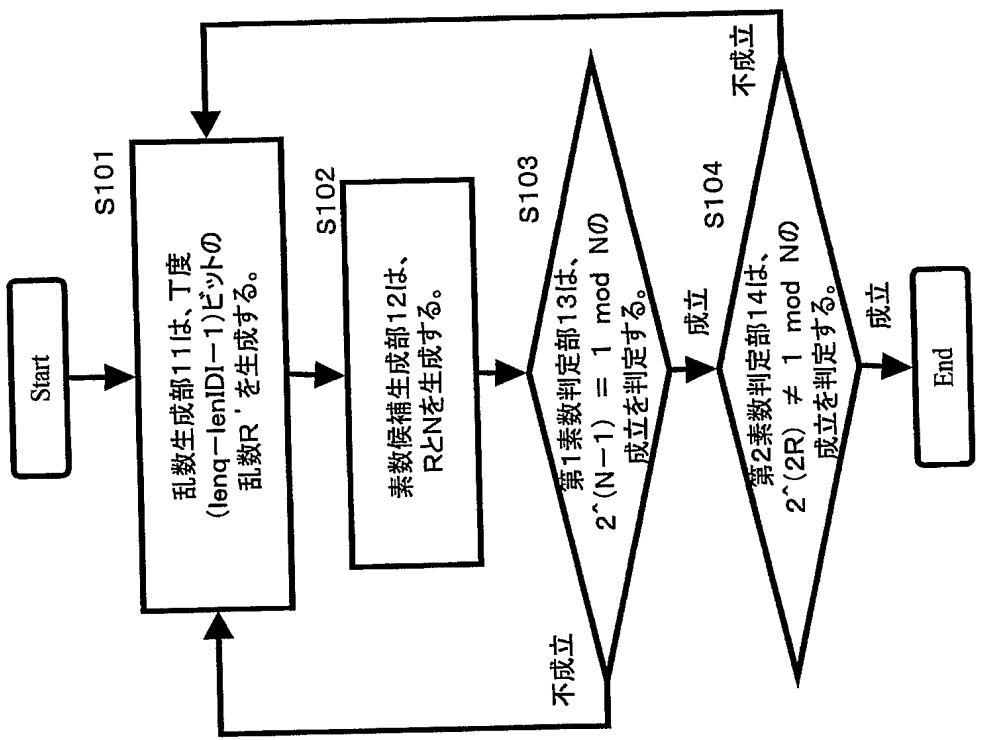
4 2 鍵発行サーバ B

- 4 3 鍵発行サーバC
- 4 4 証明書発行サーバ
- 4 4 4 発行公開鍵確認部
- 4 4 5 発行公開鍵格納部
- 4 4 6 公開鍵証明書生成部
- 4 4 7 公開鍵証明書格納部
- 4 5 i (i = 1 ~ n) 端末装置

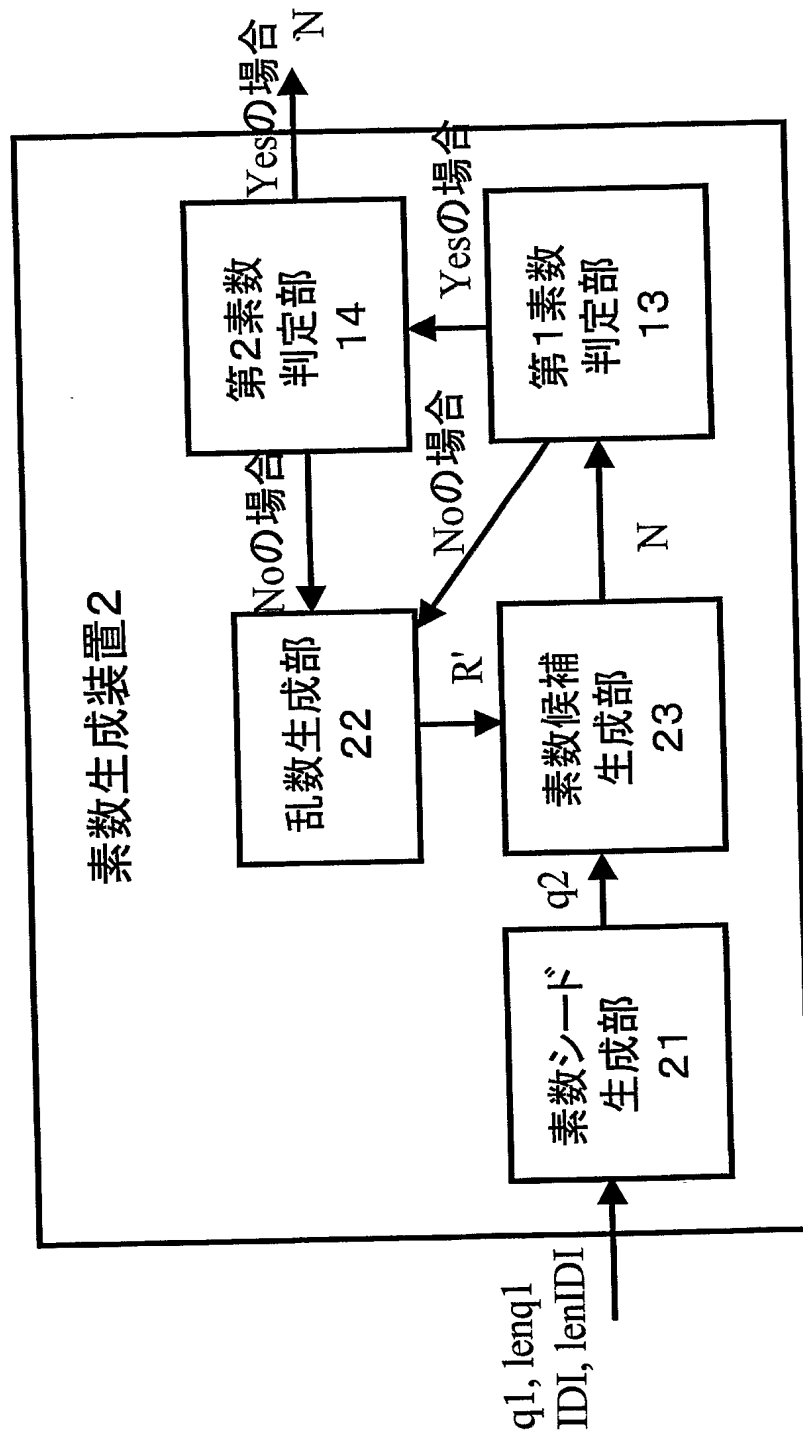
【書類名】 図面
【図 1】



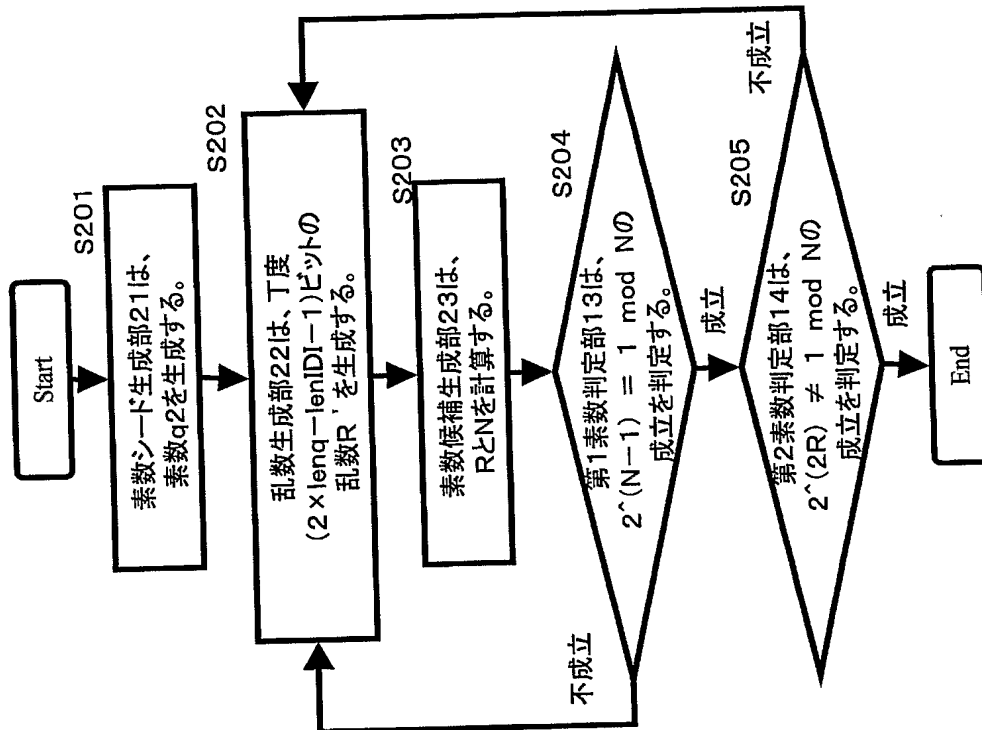
【図 2】



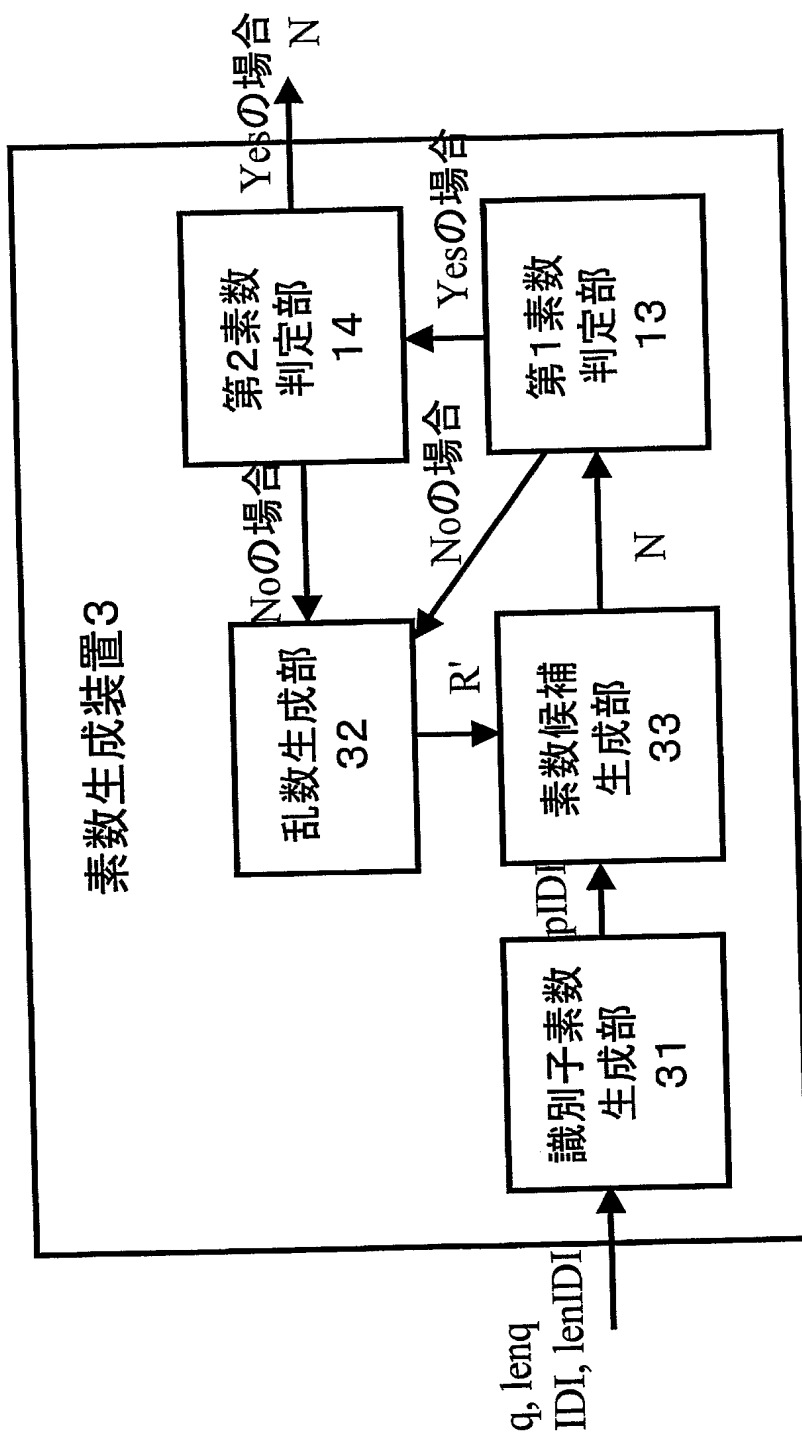
【図 3】



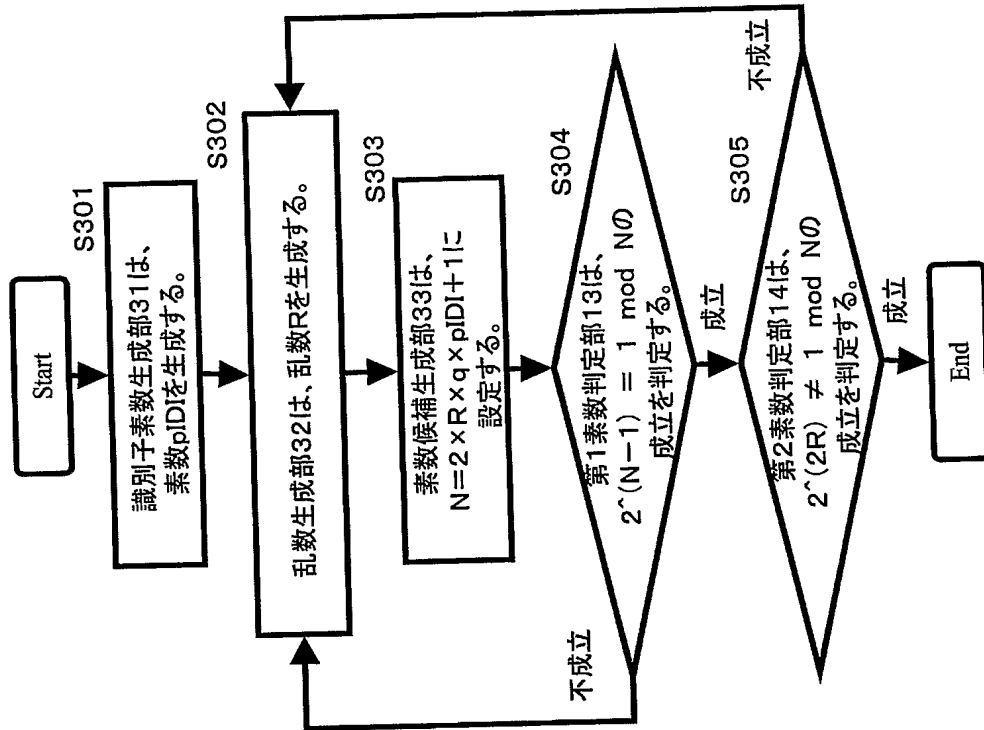
【図 4】



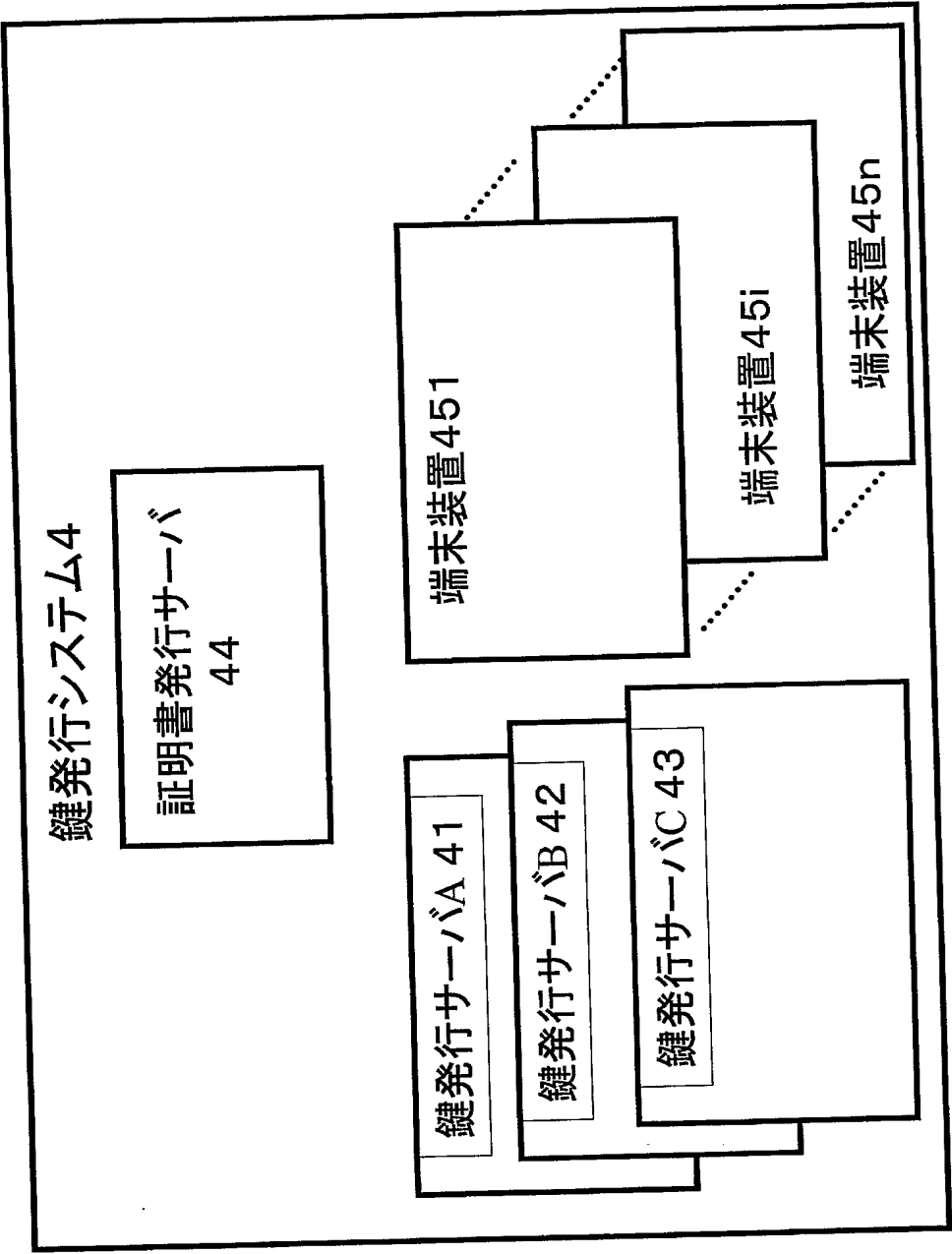
【図 5】



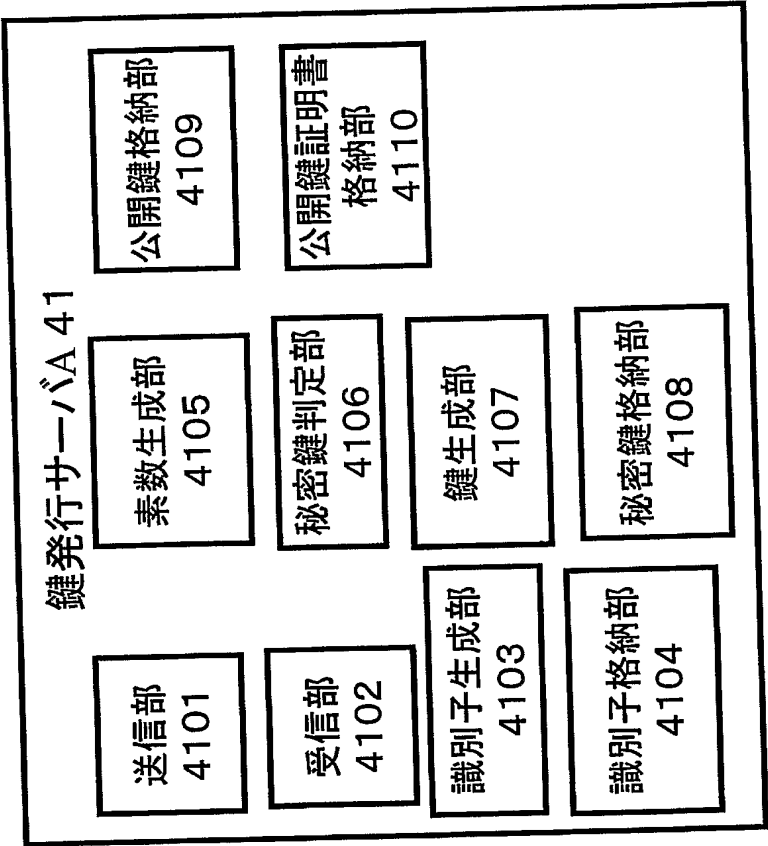
【図 6】



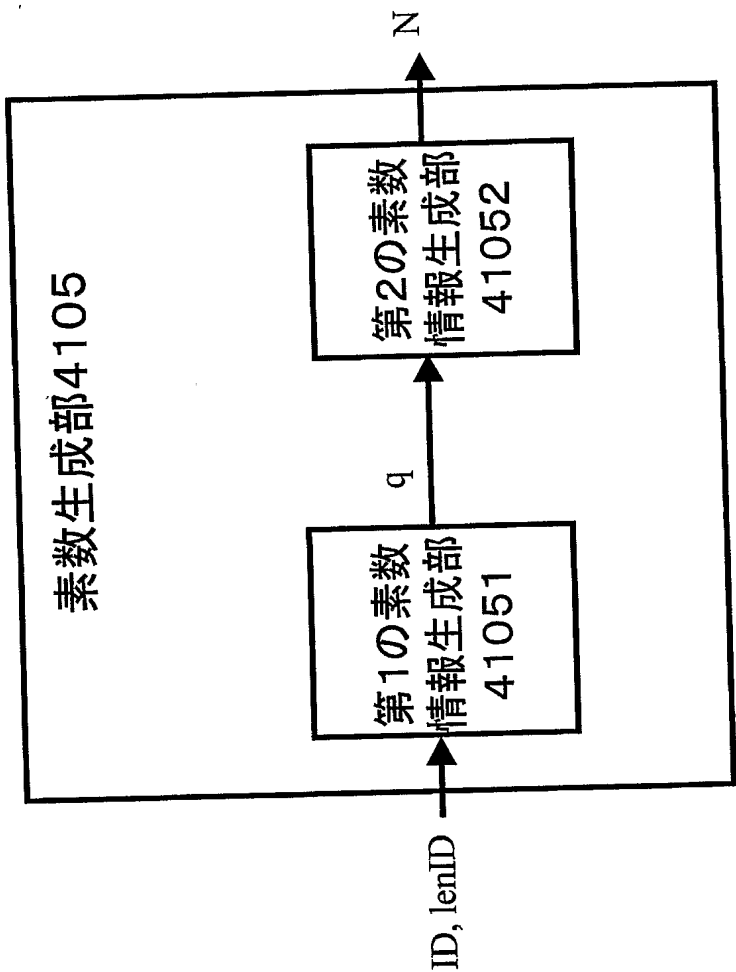
【図 7】



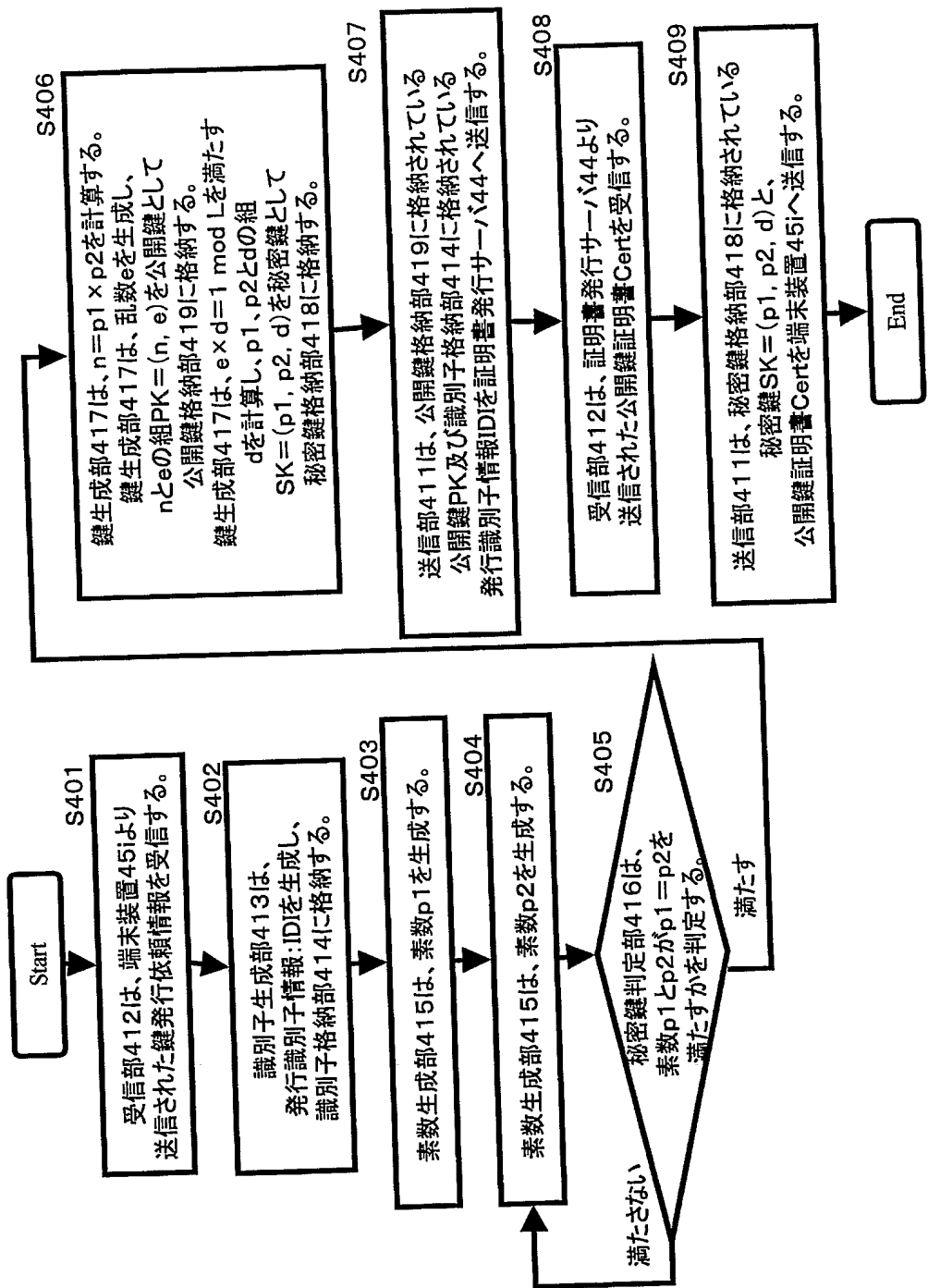
【図 8】



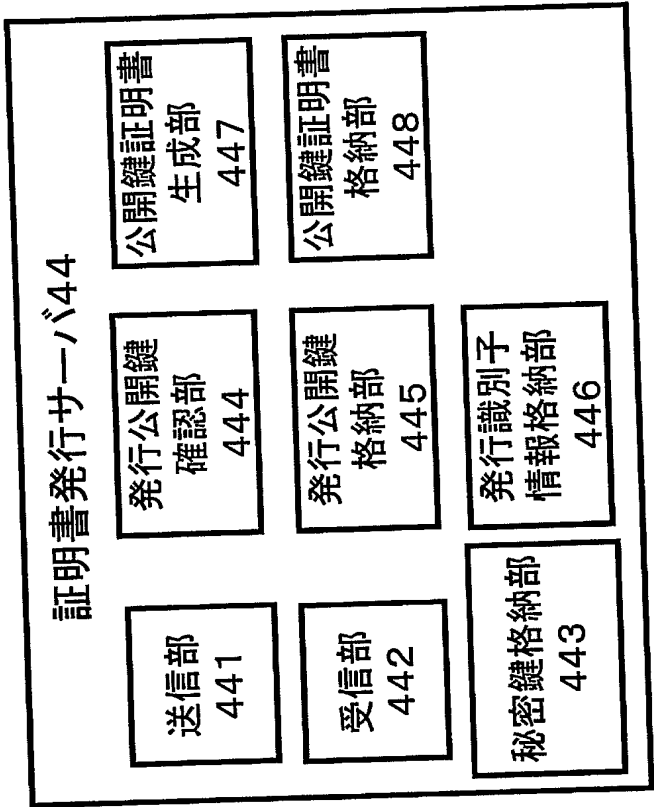
【図 9】



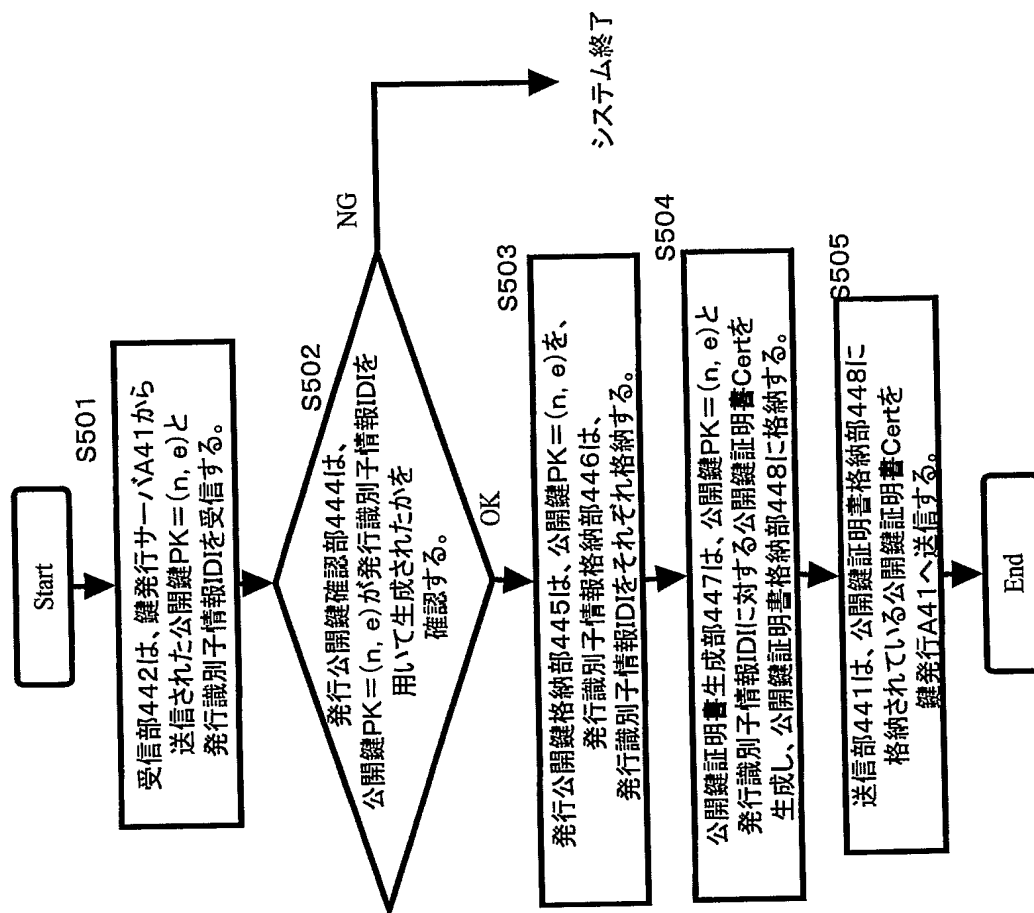
【図 10】



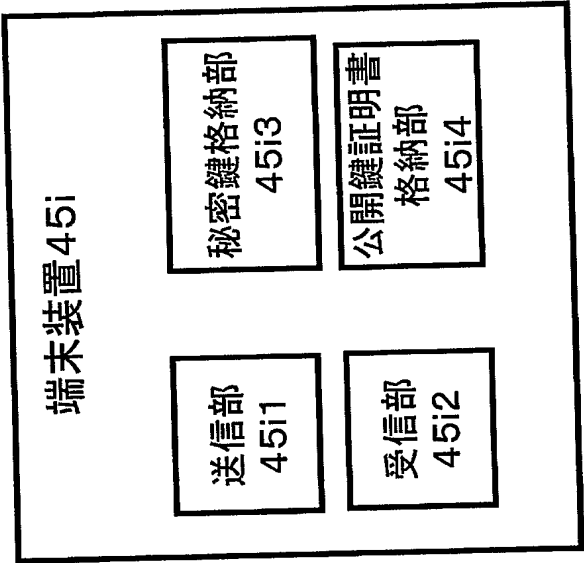
【図 1 1】



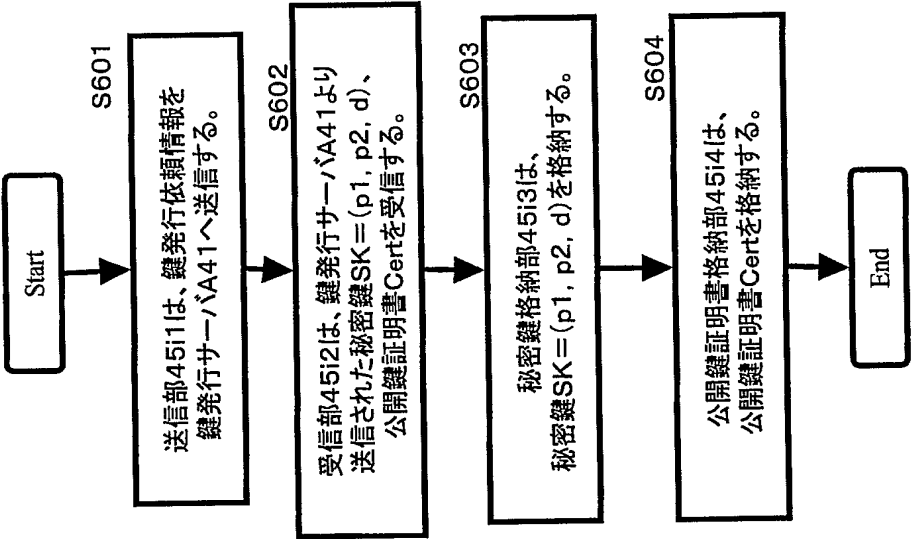
【図 12】



【図 1 3】



【図 14】



【書類名】 要約書**【要約】**

【課題】 従来技術では、複数回素数生成を行ったときに素数が一致する可能性があり、それにより、暗号の安全性を著しく低下させるという課題がある。また、生成した素数をチェックすることは、素数が増加すると困難になる。

【解決手段】 鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備える。素数に発行識別子を埋め込むことにより、発行識別子ごとに異なる素数を生成できる。

【選択図】 図 4

特願 2 0 0 3 - 4 3 3 9 0 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社